General Data Protection Regulation (GDPR)

Notes for US Educational Institutions

Key Points

- Replaces the Data Protection Directive 95/46/EC
- Harmonizes data privacy laws across Europe
- Protects and empowers all EU persons' data privacy
- Reshapes the way organizations across the region approach data privacy
- Approved by EU: **14 April 2016**
- Enforcement date: **25 May 2018**

Basic Differences

United States

- Privacy and data practices per sector
  - HIPAA :: Health data
  - FERPA :: Education
  - COPPA :: Children
  - PCI :: Credit Cards
- Can be confusing because of the number of regulations

European Union

- Consumer-oriented
- All data transactions
- Applies to all commercial and professional transactions
- Non Industry-specific
- Entire life-cycle (collection and processing) of all personal information
- Consent is a pre-condition for collections, storage, uses, matching, and disclosures

Basic Definitions

- **Data Controller** :: determines the purposes, conditions and means of the processing of personal data
- **Data Processor** :: any entity that processes personal data on behalf of the controller
- **Personal Data** :: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person
- **Consent** :: must be **explicit** for sensitive data and **unambiguous** for non-sensitive data
- **Data Protection Officer** :: a person with expert knowledge of data protection law and practices to assist the controller or processor in monitoring internal compliance with GDPR. The DPO is also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data

Basic Definitions

- **Data Protection Authorities** :: will oversee compliance, provide consultation and prior approvals, and receive and administratively adjudicate complaints against controllers and processors
- **Data Protection Impact Assessment** :: assessment to evaluate, in particular, the origin, nature, particularity and severity of a high risk to the rights and freedoms of natural persons
- **Data Processing Agreement** :: agreement between the Controller and Processor that stipulates the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data to be processed, the categories of data subjects and the obligations and rights of the controller

What kind of Data is covered?

- First and Last Name
- Bank Account information
- Address
- Medical Records
- Passport information
- Personal e-mail addresses
- Credit Card information
- Photos/videos posted on social media
- Usernames/passwords
- IP Addresses

Basic Rights

- **Breach Notification** :: must be notified within 72 hours after becoming aware of breach
- **Right to Access** :: access to their personal data and information about how these personal data is being processed
- **Right to be Forgotten** :: have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data

Basic Rights

- **Data Portability** :: have the right to receive the personal data concerning them, which they have previously provided, and have the right to transmit that data to another controller
- **Privacy by Design and by Default** :: calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. Calls for Controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing

Requirements & Policies

- Data security practices
- Personal data usage and privacy restrictions
- Data breach reporting requirements
- Personal data consent collection requirements

Sanctions

a. a warning in writing in cases of first and non-intentional non-compliance
b. regular periodic data protection audits
c. a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Lower Level)
d. a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Upper Level)

Does it affect you?

- GDPR has an increased territorial scope
- If your organization is either offering goods or services to data subjects or monitoring the behavior of data subjects while they are located within the EU, you do qualify as a data controller under the rule.
- Some examples:
  - Applications from EU residents
  - Admissions from EU residents
  - Online learners living in EU countries
  - Alumni or donors based in the EU
  - Marketing communications recipients

Do you need a Data Protection Officer?

- You must have a DPO if you are one of the following:
  - A Public Authority
  - An organization that engages in large scale systematic monitoring
  - An organization that engages in large scale processing of sensitive personal data

- Characteristics
  - Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
  - May be a staff member or an external service provider
  - Contact details must be provided to the relevant DPA
  - Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
  - Must report directly to the highest level of management
  - Must not carry out any other tasks that could results in a conflict of interest.

Don’t Panic … Yet

If you already have the controls below in place to help with PCI, GLBA, HIPAA, FERPA you are on your way to GDPR compliance:

a. Personal data processed by the organization should be relevant and limited to only what is necessary.

b. Secure all systems used for processing personal data to prevent unauthorized access. Networks and information systems used should be secured to prevent accidental events and malicious actions that compromise the availability, integrity, and confidentiality of stored or transmitted data. The GDPR specifically mentions securing electronic communications networks and protecting them from malicious code distribution.

c. Ensure the period for which the personal data is stored is limited to a strict minimum. Data retention policies should be established and periodically reviewed.

Consider doing a Data Impact Risk Assessment

- You want answers to the following questions:
  - What data is being collected?
  - Where is the data being sourced?
  - Why is the data collected?
  - How is it processed?
  - Who has access?
  - How long is the data retained?
  - Where is the data transferred to?
  - Is data used in accordance of collection consent?

Some Key Stakeholders

- Chief Information Security Officer
- Chief Privacy Officer
- General Counsel
- Internal Audit
- Admissions
- Registrar
- Study Abroad Office
- International Employment Affairs Office
- Distance Learning
- Office of Communications
- Research Office

Good References

- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- https://www.eugdpr.org
- https://er.educause.edu/articles/2017/8/the-general-data-protection-regulation-explained
- https://www.campusguard.com/public/NewsArticle-2018.01.09-GDPR.pdf